MINUTES OF THE JUNE 26, 2013 MEETING
OF THE BREACH RESPONSE PROTOCOL WORKGROUP

The Breach Response Workgroup ("Workgroup") held a meeting at 1:30 p.m. on June 26, 2013, at the State of Illinois James R. Thompson Center, 100 W. Randolph Street, Chicago, IL 60601

In attendance:

Laurel Fleming (Co-Chair)
David Miller (Co-Chair)
Khadine Bennett
Karen Beyer (via telephone)
Victor Boike
Ryan Gehbauer
Deb Gory (via telephone)
Deborah Hayes
Jim Hammer
Susan O'Keefe
Ivana Sreckov
Kerri McBride (ILHIE Staff)
John Saran (ILHIE Staff)

Other Committee members

Dr. Monique Anawis
Charles (Chuck) Cox
Dana Crain
Jud Deloss
Mikki Pierce
Jodi Sassana
Ivan Sergeev
Michael Short

Kerri McBride, Legal Counsel for ILHIE/OHIT and Staff Liaison for the Workgroup, called the meeting to order at 1:32 p.m. Introductions of committee members present (in person and by telephone) followed.

Report on New Rule by HHS

As an initial matter, Kerri McBride and John Saran advised the Workgroup that HHS has proposed a new rule with regard to FFEs (Federally Funded Insurance Exchanges) which would require the reporting of a breach or security incident to HHS within the hour. A link to the proposed rule will be sent to the Workgroup. John Saran noted that under the rule, wherever the breach incident occurs, that entity has to take full responsibility of the management, coordination, mitigation, etc. of the breach response.

Project Management

Laurel Fleming described the purpose of the Workgroup, which is to develop a breach protocol. A draft of a protocol, developed by Kerri McBride and John Saran, was provided in the meeting packet as a way to elicit questions and start the discussion. The Workgroup is expected to finalize a protocol and submit it to the Data Security and Privacy Committee ("DSPC"), by mid-September. The DSPC meetings are scheduled on an as needed basis. On receipt, the DSPC will review, and if necessary, revise. Once all revisions are necessary, it will be submitted to the Authority Board for consideration at its

November meeting. The finalized protocol will be an appendix to the data sharing agreement.

Participants in the drafting process

Several entities should be included in the drafting of the breach response protocol, most of which are currently represented in the Workgroup – hospitals, large providers, small providers, other HIEs, consumers. To the extent that necessary groups are not participants, time should be made during the drafting process so that input may be received from these other entities.

Review of Materials

David Miller described the handouts given before the meeting: the Draft ILHIE Breach Notification Protocol, Breach Scenarios, State HIE Breach Notification Policy Best Practices Matrix and Related Links, and the HHS Summary Breach Notification Requirements. It was decided to allow members time to examine the Best Practices Matrix and the HHS Summary, so they can be discussed at future meetings.

Discussion of Breach Scenarios

As the Workgroup proceeded to discuss breach scenarios, the following assumptions were recognized:

- In discussing breach scenarios, the Workgroup would not discuss who decides whether or not a breach has occurred or upon what basis;
- The group reviewed a diagram showing the flow of PHI from a “requesting or recipient entity” to a “source entity.” As well, PHI could flow through a regional health information organization (“RHIO”);
- ILHIE will not retain PHI, although it will aggregate and transmit PHI;
- It was noted that by 2014, most organizations and providers will be able to download requested health records into their EHR as part of complying with Meaningful Use Stage 2. At this time, many providers are able to screen print the records. Accordingly, the Workgroup would accept the premise that PHI could be transferred to and retained by the recipient entity.

The Workgroup had a lengthy and animated discussion of what should happen when a breach occurs. There was general agreement that if a provider (a covered entity) requests data through the ILHIE and there is a breach at the requesting provider’s “end,” then it is the requesting provider’s breach to manage. It is the requesting entity’s responsibility to know who has access to information obtained through the ILHIE and that it is being accessed appropriately and that there are appropriate safeguards. For example, if an employee at a hospital requests PHI through the ILHIE, brings the PHI into the hospital’s EHR, and creates a breach, it is the requesting hospital’s breach. Even so, the Workgroup also agreed that while the breach is the recipient entity’s responsibility, ILHIE and the Source entities should be notified. Kerri McBride noted that the ILHIE is a business associate of the covered entities using the ILHIE and thus may have notification responsibilities back to the source entity- - even if the requesting (breaching) entity would not have to otherwise notify the source entity under HIPAA. Thus, action may not need to be taken by all the parties involved, but all should be notified.

Further discussion related to what happened if the requester was not treating the patient currently. Two scenarios were discussed: (i) the requesting entity was consulting or reviewing the file for an upcoming appointment, or (ii) someone at the requesting entity was accessing the data for an inappropriate reason (a voyeuristic breach). In those situations, who "owns" the breach for notification purposes?

With respect to the first issue, the Workgroup discussed whether there is a way to limit access to entities which have a current or upcoming treatment relationship with the patient whose data is requested. This issue and a couple of other questions relating to technical aspects of the ILHIE led to the suggestion that the CTO or other technical resource be available for questions at one of the next few meetings.

In discussing voyeuristic breaches, the issue of monitoring access was raised. Should entities participating in ILHIE be required to audit their respective EHRs to detect inappropriate accesses? The Workgroup concluded that while auditing may be an important to the ILHIE, audit requirements are more appropriated addressed in the Patient Consent Preferences and Data Security Workgroup.

If the ILHIE is breached, it must notify any participant whose data was breached, as well as any data contributors. If the data is still sent to the recipient in this case, the recipient must also be notified of the breach. There must be coordination among the data contributors involved if a notification of the breach needs to be published, and in such a case, the organization responsible for the breach should have the most influence on the publication and is primarily responsible for notification. If the breach occurs by an organization that did not have the patient relationship, the organization with the relationship may want to be involved. The language of the notification should be acceptable to all the sources involved. The Workgroup agreed that ILHIEA should coordinate between all affected parties notification and other breach related issues.

Moving Forward

The Workgroup will continue to talk about breach scenarios. Workgroup members were asked to review and provide comments or edits to the current draft protocol for the next meeting. Ground rules for handling a breach should be developed in the future. A review of the best practices matrix and other HIE policies would be helpful to increase the group's background knowledge. To the extent they are available, they will be sent to the group prior to the next meeting. The meeting schedule for the next 6 weeks was set as shown below. Initially, all meetings will be 90 minutes and convene at 10:00 am. The Workgroup agreed to meet face to face on a monthly basis as it may help to move the process along.

Meeting Schedule

July 9, 16, 23 (face to face), 30, August 6 and 13.

Adjournment

The meeting was adjourned at 2:31 p.m.